The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/14/2017

SUBJECT:
Cumulative Security Update for Microsoft Edge (MS17-007)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Edge, the most severe of which could allow remote code execution if a user views a specially crafted web page. Microsoft Edge replaced Internet Explorer as the default browser on Windows 10. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Microsoft Windows 10
- Microsoft Windows Server 2016

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft Edge, the most severe of which could allow for remote code execution if a user views a specially crafted web page. Details of these vulnerabilities are as follows:
- Multiple remote code execution vulnerabilities exist in the way affected Microsoft scripting engines render when handling objects in memory. (CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-

2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, CVE-2017-0151)

- A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. (CVE-2017-0037)
- A remote code execution vulnerability exists when Microsoft Windows PDF Library improperly handles objects in memory. (CVE-2017-0023)
- A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. (CVE-2017-0034)
- Multiple information disclosure vulnerabilities exist in the way that the affected components handle objects in memory. (CVE-2017-009, CVE-2017-0011, CVE-2017-0017, CVE-2017-0065, CVE-2017-0068)
- Three spoofing vulnerabilities exist when a Microsoft browser does not properly parse HTTP responses. (CVE-2017-0012, CVE-2017-0033, CVE-2017-0069)
- Three security feature bypass vulnerabilities exist when Microsoft Edge fails to correctly apply Same Origin Policy for HTML elements present in other browser windows. (CVE-2017-0066, CVE-2017-0135, CVE-2017-0140)

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/library/security/ms17-007.aspx

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0009
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0010
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0011
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0012
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0015
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0017
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0023
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0032
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0033

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0034
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0035
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0037
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0065
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0066
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0067
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0068
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0069
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0070
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0071
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0094
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0131
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0132
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0133
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0134
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0135
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0136
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0137
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0138
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0140
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0141
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0150
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0151